21. (Currently amended) A method of operating a portable computer, comprising:

a) storing records of events experienced by the computer in user-accessible memory within the computer;

b) using ~~some~~ one or more of the records as seed for generating plain text of a first session key K1; and then

c) encrypting K1, transmitting K1(encrypted) to an external terminal, receiving an encrypted response from the external terminal, and de-crypting the encrypted response using the plain text of K1.

22. (Previously added) Method according to claim 21, and further comprising:

d) repeating processes of paragraphs (a) and (b) to produce a second session key K2, different from the first session key K1; and

e) using K2 in a transaction with an external terminal.

23. (Previously added) Method according to claim 21, wherein the records used as seed include at least one element selected from the following group:

1) recorded button selections,

2) recorded pointer movements,

3) recorded data entered by a user,

4) current date setting, and

5) current time setting.

24. (Previously added) A method, comprising:

a) using a portable computer to

i) generate a first session key K1, based on one or more seeds derived from data contained in user-accessible memory;

ii) encrypt K1 into K1(encrypted), using a public key PK;

iii) transmitting K1(encrypted) to an external terminal in connection with a first transaction;

b) using the portable computer to

i) generate a second session key K2, based on one or more seeds derived from data contained in user-accessible memory;

ii) encrypt K2 into K2(encrypted), using a the public key PK;

iii) transmitting K2(encrypted) to an external terminal in connection with a second transaction.

25. (Previously added) Method according to claim 24, wherein the data from which as the seeds are derived include at least one element selected from the following group:

1) recorded button selections,

2) recorded pointer movements,

3) recorded data entered by a user,

4) current date setting, and

5) current time setting.

26. (Previously added) Method according to claim 24, and further comprising:

c) in connection with the first transaction,

i) receiving into the portable computer an encrypted message EM1 from the external terminal, and

ii) de-crypting EM1 using K1.

27. (Previously added) Method according to claim 26, and further comprising:

d) in connection with the second transaction,

i) receiving into the portable computer an encrypted message EM2 from the external terminal, and

ii) de-crypting EM2 using K2.

28. (Previously added) A method, comprising:

a) maintaining a commercially available Personal Digital Assistant, PDA, which has no secure area for storing an encryption key usable to encrypt outgoing data; and

b) using the PDA for encryption and transmission of a message to an external controller in connection with a financial transaction.

29. (Previously added) Method according to claim 28, wherein the encryption comprises

a) deriving a seed from data stored in user-accessible memory; and

b) deriving a session key from said seed, which session key is used in the financial transaction, and not used thereafter.

30. (Previously added) Apparatus, comprising:

a) a portable computer having

i) no secure area for storing an encryption key used to encrypt outgoing data;

ii) system memory, all of which is accessible to a user of the computer; and

iii) data stored in the system memory, which data changes over time;

b) means for

i) utilizing selected changing data in the system memory as a seed for generating a session key K1;

ii) encrypting K1 into K1(encrypted); and

iii) transmitting K1(encrypted) to an external terminal.

31. (Previously added) Apparatus according to claim 30, wherein the data used as the seed includes at least one element selected from the following group:

1) recorded button selections,

2) recorded pointer movements,

3) recorded data entered by a user,

4) current date setting, and

5) current time setting.

32. (Previously added) Apparatus according to claim 31, and further comprising:

c) means for

i) receiving an encrypted message from the external terminal, and

ii) de-crypting the encrypted message using K1.

33. (Currently amended) A portable computer, comprising:

a) means for storing records of events experienced by the computer in user-accessible memory within the computer;

b) means for using ~~some~~ one or more of the records as a seed for generating an encryption key; and

c) means for using the encryption key in a transaction with an external terminal.

34. (Previously added) Method according to claim 33, wherein the records used as the seed include at least one element selected from the following group:

1) recorded button selections,

2) recorded pointer movements,

3) recorded data entered by a user,

4) current date setting, and

5) current time setting.

35. (Previously added) Method according to claim 21, wherein the portable computer requires entry of a Personal Identification Number, PIN, prior to generation of the encryption key, and will not complete the transaction without the PIN.

36. (Previously added) Method according to claim 24, wherein the portable computer requires entry of a Personal Identification Number, PIN, prior to generation of the encryption key, and will not complete the transaction without the PIN.

37. (Previously added) Method according to claim 26, wherein the portable computer requires entry of a Personal Identification Number, PIN, prior to encryption, and will not complete the transaction without the PIN.

38. (Currently amended) A method, comprising:

a) storing records of events experienced by a portable computer in user-accessible memory within the computer;

b) using ~~some~~ one or more of the records as a seed for generating a session key K1;

c) encrypting K1 into K1(encrypted) using a public key;

d) transmitting K1(encrypted) to an external terminal;

e) at the external terminal, decrypting K1(encrypted) into K1;

f) encrypting a message M into M(encrypted) using K1 as key;

g) transmitting M(encrypted) to the portable computer; and

h) decrypting M(encrypted) using K1 within the portable computer.